IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF: AN APPLE IPHONE, BLACK IN COLOR, INSIDE A CLEAR CASE; AND AN APPLE IPHONE MINI, BLACK IN COLOR, INSIDE A BLACK LEATHER CASE, CURRENTLY LOCATED IN THE EVIDENCE STORAGE ROOM AT 324 25th STREET, OGDEN, UT 84401	Case Nos. 2:23-mj-00140 DBP

AFFIDAVIT IN SUPPORT OF APPLICATIONS UNDER RULE 41 FOR WARRANTS TO SEARCH AND SEIZE

I, Matthew Curtis, being duly sworn upon oath, hereby declare as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of and the extraction of electronically stored information from two devices —that is, an Apple Iphone, black in color, inside a clear case, that was recovered on December 8, 2022, from the personal possession of defendant MAKAIO LYMAN CRISLER ("CRISLER") at the time of his arrest; and an Apple Iphone mini, black in color, inside a black leather case, that was recovered on December 8, 2022 from the personal possession of defendant RICHARD SCOTT NEMROW ("NEMROW") at the time of his arrest —which are currently in the possession of law enforcement (hereinafter, the "Devices").

2. I am a Special Agent with IRS Criminal Investigations (IRS-CI). I have been a Special Agent with IRS-CI for 19 years, and am currently assigned to the Ogden, Utah post of duty for the Phoenix Field Office. I have a master's degree in Business Administration and have received extensive training in financial investigative techniques and have investigated possible

criminal violations of the Internal Revenue Laws (Title 26, United States Code), the Bank Secrecy Act (Title 31, United States Code), Money Laundering Statutes (Titles 18 and 31, United States Code), and violations of other federal statutes. I work in coordination and collaboration with numerous other agencies and law enforcement departments in enforcing and investigating federal crimes, and am certified to author search warrant affidavits. I have participated in numerous search warrants, and have experience in searching for materials including business records, bank records, currency and other monetary instruments, and other documents evidencing efforts to obtain, secret, and conceal assets by individuals or business entities. In addition, I have experience in obtaining search warrants to examine the contents of electronic devices in connection with criminal investigations.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other officers, agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

II. JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

III. IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. I make this affidavit in support of applications for warrants to search the following devices, which are currently in the possession of law enforcement in the evidence storage room at 324 25th Street, Ogden, UT 84401:

a. An Apple Iphone, black in color, inside a clear case, recovered from defendant CRISLER at the time of his arrest on December 8, 2022, and which phone was used by CRISLER at the time of his arrest to contact his wife, as more fully described in Attachment A; and

b. Apple Iphone mini, black in color, inside a black leather case, recovered from the pocket of defendant NEMROW at the time of his arrest on December 8, 2022, and which phone had, inside the case, cards belonging to defendant NEMROW, as more fully described in Attachment A.

(collectively, the "Devices") for evidence, fruits, and instrumentalities of criminal offenses, including but not limited to, violations of 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1957 (Money Laundering); 18 U.S.C. § 1343 (Conspiracy to Commit Wire Fraud, and Wire Fraud), and 18 U.S.C. § 1028A (Aggravated Identity Theft). The applied-for warrants would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

6. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 1344 (Conspiracy to Commit Bank Fraud), 18 U.S.C. § 1957 (Conspiracy to Commit Money Laundering); 18 U.S.C. § 1343 (Wire Fraud), and 18 U.S.C. § 1028A (Aggravated Identity Theft), have been committed by defendants CRISLER and NEMROW, as well as their co-defendants and others. There is also probable cause to search the Devices, further described below and in Attachment A, for the things described in Attachment B.

IV. PROBABLE CAUSE

7. On December 7, 2022, a federal grand jury returned an indictment in case number 2:22-cr-00481-CW charging defendants CRISLER and NEMROW, along with seven (7) other defendants (hereinafter, the "charged defendants"), with violations of 18 U.S.C. § 1344 (Conspiracy to Commit Bank Fraud), 18 U.S.C. § 1343 (Conspiracy to Commit Wire Fraud, and

Wire Fraud), 18 U.S.C. § 1957 (Conspiracy to Commit Money Laundering), and 18 U.S.C. § 1028A (Aggravated Identity Theft).

8. The criminal violations charged in the indictment are predicated on the charged defendants' participation in interrelated fraud and money laundering conspiracies to obtain more than $100,000,000 of credit and debit card processing from financial institutions and payment processors. The charged conspiracies took place over a period of almost six years and continued through at least April 2022.

9. The scheme involved the sale of nutraceutical, CBD, and dietary supplement products to consumers through a number of websites and a call center operating in Utah. All of the sales required the consumer to provide a credit or debit card, which card was billed through a credit or debit card processing transaction.

10. The nutraceutical, CBD, and dietary supplement products were advertised to consumers as providing benefits such as weight loss and the treatment of seizures, cancers, and erectile dysfunction, and included false claims about the products' effectiveness and false celebrity endorsements. Consumers were also misled about the price of products and the ability to return or to obtain a refund for the product.

11. The sale of nutraceutical, CBD, or dietary supplement products is considered high risk for financial institutions and payment processors who process credit card transactions ("Merchant Processors") because of the large numbers of chargebacks, liability associated with consumer use of the products, potential false marketing often associated with these products, the potential of facilitating or funding criminal activity, and potential reputational and financial harm to the Merchant Processor. Merchant Processors attempt to limit their risk and liability in relation

to these types of high-risk businesses by engaging in underwriting and other practices before and after a merchant account is opened.

12. In an effort to avoid the risk-mitigating actions taken by Merchant Processors and to facilitate the tens of thousands of misleading online sales transactions to acquire more than $100,000,000, the charged defendants, with the assistance of others, set up hundreds of sham limited liability companies (LLCs), created and used hundreds of false and misleading websites to act as "false storefronts" for the sham LLCs, and set up hundreds of business checking accounts and merchant processing accounts in the names of others, but which the charged defendants controlled. The charged defendants recruited and paid individuals (herein "straw owners") for the use of their personal information to create the sham LLCs, and open business checking accounts and merchant processing accounts for the sham LLCs through which the charged defendants processed the sales of their products and transferred the proceeds to benefit themselves and others involved in the scheme.

13. As part of the scheme, the charged defendants regularly manipulated sales transactions to keep the merchant accounts for the sham LLCs open as long as possible. Merchant accounts were suspended or closed by Merchant Processors when the percentage of transactions resulting in chargebacks was too high. The charged defendants conducted thousands of false sales transactions using prepaid gift cards to lower the chargeback rate in an effort to keep the merchant accounts open. The charged defendants referred to these false sales transactions as "friendlies." A typical "friendly" transaction involved the use of a prepaid gift card for a low dollar "sale" of a product. The consumer information for the "sale" was falsified and no product was shipped or provided to anyone.

14. In addition, as part of the scheme, the charged defendants customized and used a customer relationship management software program ("CRM") to further and to conceal the scheme. Specifically, the CRM aided the charged defendants by distributing sales of products across multiple merchant accounts in the names of the sham LLCs. The CRM was also designed to aid in the processing of "friendly" transactions. The CRM was modified to inform the charged defendants when a sale of product was attempted or made through one of the false storefront websites submitted to Merchant Processors so the charged defendants could take additional steps to conceal their scheme. The CRM was also modified to allow the charged defendants to manipulate the on-line websites through which they made sales to consumers. Specifically, the CRM allowed the charged defendants to "hide" pricing and subscription information so that consumers were not able to see that, by purchasing a product on the website, they were automatically enrolled in a subscription service that charged their credit and debit cards on a recurring basis.

15. Defendants CRISLER and NEMROW controlled Target Fulfillment LLC, which was registered in Utah as a foreign limited liability company, with its principal place of business located in Utah.

16. The charged defendants used Target Fulfillment LLC as the entity that fulfilled and managed the sales of the products in the scheme. Target Fulfillment LLC processed the sales orders from consumers and used the CRM to distribute sales across multiple merchant accounts to further and conceal the scheme. In addition, bank accounts controlled by Target Fulfillment LLC were used to "layer" proceeds from the scheme to benefit the charged defendant.

17. The charged defendants also used Total Client Connect, DBA for Elite Business Resources LLC, as the entity through which the charged defendants operated a call center in

Utah that was designed to further the scheme. In addition, bank accounts in the name of Energia LLC and Control Marketing LLC were used by the charged defendants to "layer" proceeds from the scheme to benefit the charged defendants. Defendant CRISLER controlled Energia LLC.

18. In April 2018, approximately two years into the charged conspiracies, defendant NEMROW and co-defendant PHILLIP GANNUSCIA were permanently enjoined by the Federal Trade Commission from, among other things, making or assisting others in making any false or misleading statement to obtain payment processing services. The injunction also prohibited defendants NEMROW and GANNUSCIA from engaging in any tactics to avoid fraud and risk monitoring programs by any Merchant Processor, including tactics such as balancing or distributing sales transactions among multiple merchant accounts or using shell companies to apply for a merchant account. I have reviewed the injunction order issued by the U.S. District Court for the District of Utah.

19. As a result of the permanent injunction imposed by the Federal Trade Commission, the charged defendants attempted to conceal the role played by defendants NEMROW and GANNUSCIA by placing the ownership of Target Fulfillment LLC in defendant CRISLER's name only. However, information provided by multiple witnesses, including those employed by Target Fulfillment, as well as numerous email communications, and other electronic evidence, demonstrate that defendants NEMROW and GANNUSCIA played an integral and controlling role in both Target Fulfillment LLC and in the fraudulent efforts to obtain merchant processing accounts.

20. Evidence about the above-described scheme, how it worked, and the involvement of the charged defendants was obtained by law enforcement from, among other things, the following: (1) interviews with more than twenty (20) of the straw owners; (2) the review of

hundreds of merchant processing account applications; (3) the review of thousands of electronic records and communications between the charged defendants, which was obtained from the execution of a Google search warrant in 2022; (4) interviews with multiple employees who worked for the charged defendants and/or business entities involved in the scheme to include Target Fulfillment LLC; (5) interviews with participants in the scheme, to include several charged defendants, and uncharged individuals; and (6) the review of thousands of pages of bank records from hundreds of bank accounts.

21. The straw owners consistently reported to law enforcement that they were recruited by a charged defendant(s) to open a sham LLC for the purpose of allowing the charged defendants to use the sham LLC to sell products. The straw owners signed paperwork to open a bank account for the sham LLC, but control of that bank account was given to one of the charged defendants. The straw owners were paid a nominal amount, usually $250-$350/month, as long as their merchant account remained open. The straw owners did nothing to operate the businesses, made no decisions related to the businesses, and had little to no knowledge of the businesses. In addition, when shown applications to open merchant processing accounts and corporate agreements that they purportedly signed, numerous straw owners reported that they never signed, authorized, or had any knowledge about the documents. At least one straw owner was advised by a charged defendant that the reason their merchant accounts were only open for a short period of time is because the way in which the charged defendants conducted business was a little shady and the banks would eventually close the accounts.

22. A review of the merchant processing account applications submitted for the sham LLCs reveals that all of the applications were submitted to the Merchant Processors electronically, with electronic signatures purportedly signed by the straw owners. Electronic

devices were used to prepare, sign, and submit each of these applications. In addition, an email address for each sham LLC was set up and controlled by at least one of the charged defendants.

23. A review of the electronic records obtained in the Google search warrant reveals that defendant CRISLER and defendant NEMROW regularly used electronic devices to communicate with others for the purpose of monitoring the chargeback rates, directing the use of "friendlies" and the spreading of sales across merchant processing accounts, and monitoring the opening and closing of merchant processing accounts to further the scheme. For example, as it relates to "friendlies," in a January 20, 2018 email, defendant CRISLER instructs an employee to add two merchant processing accounts from sham LLCs to the "40 a day friendly rotation." (During an interview with law enforcement, that employee described how they were directed by defendants CRISLER and NEMROW to routinely engage in processing "friendly" transactions to try to keep the merchant accounts open.) On December 11, 2018, co-defendant BRENT KNUDSON emailed defendant NEMROW advising that they need to run "friendlies" on a specific merchant processing account that was experiencing high chargebacks. On May 28, 2020, defendant CRISLER emailed defendant NEMROW a copy of an inquiry regarding certain disputed charges and the increased number of chargebacks for one of the sham LLC merchant processing accounts. Specifically, Defendant CRISLER forwarded the inquiry to defendant NEMROW and advised that he (CRISLER) deactivated the account in the CRM but that "I don't think keeping it taking friendlies is a bad idea, . . ."

24. The review of electronic documents from the Google search warrant also reveals that Defendants CRISLER and NEMROW were regularly informed, via electronic mail, when a merchant processing account was being closed due to high chargeback rates. For example, on February 14, 2020, co-defendant BRENT KNUDSON forwarded to defendants CRISLER,

NEMROW, and GANNUSCIA the closure notification for eleven (11) different merchant processing accounts assigned to sham LLCs due to a high chargeback ratio.

25. During interviews with witnesses, to include employees of Target Fulfillment LLC, and other participants in the scheme to include other co-defendants, the witnesses described the scheme, how it operated, and the role of defendants CRISLER and NEMROW. The witnesses' descriptions are consistent with the statements made in paragraphs 8 through 18 of this affidavit. In addition, multiple witnesses described how they were directed by defendant CRISLER to transfer money to and from various bank accounts (including the sham LLC bank accounts) for purposes of layering the proceeds from the scheme.

26. During the course of the investigation, your affiant observed a video taken with a cell phone of a meeting between several charged defendants and others. Defendants GANNUSCIA, BOBBY JO JACKSON, NEMROW, and CRISLER are present in the meeting. During the meeting, co-defendant GANNUSCIA admits that they were engaged in money laundering.

27. Your affiant was also informed by multiple witnesses, including two co-defendants, that they regularly communicated with defendants via electronic mail, text message, and encrypted apps. Your affiant was also advised by a co-defendant that they had numerous text messages on their cell phone from others involved in the scheme, to include defendant CRISLER. In addition, your affiant knows from multiple witnesses, including two co-defendants, that several of the charged defendants reside out of state and/or in other parts of the State of Utah from where NEMROW and CRISLER reside and work, making communication through electronic devices necessary to coordinate the scheme.

28. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know that the Devices are capable of and frequently used to communicate with other individuals, take and store photographs and videos, and used for internet searches, among other things. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device (and sometimes by implication who did not), as well as evidence relating to the commission of the offenses under investigation. For example, in my training and experience, individuals involved in conspiracies to commit bank fraud, wire fraud, and money laundering frequently communicate with others using electronic devices about their criminal scheme. In this case, I have reviewed hundreds of electronic communications between the charged defendants, to include communications to or from defendants CRISLER and NEMROW, to further the scheme. I have also interviewed multiple witnesses who stated that they communicated with the charged defendants through encrypted apps, text communications, and other electronic communications.

29. The Devices are currently in the lawful possession of law enforcement. They came into law enforcement's possession as part of a search incident to the separate arrests of defendant CRISLER and defendant NEMROW on December 8, 2022, which arrests were authorized after the return of the indictment in case number 2:22-cr-00481-CW. I seek the additional warrants out of an abundance of caution to be certain that an examination of the Devices complies with the Fourth Amendment and other applicable laws.

30. The Devices are currently located in a law enforcement evidence storage room located at 324 25th Street Ogden, UT 84401. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this

investigation, in substantially the same state as they were when the Devices first came into the possession of law enforcement.

V. TECHNICAL TERMS

31. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images.

Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

32. Based on my training, experience, and research, I know that the Devices have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and/or PDA, and that it can access the Internet.

VI. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

33. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

34. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

35. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit the examination of the Devices consistent with the warrants. The examination may require authorities to employ techniques,

including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

37. *Manner of execution.* Because the warrants seek only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

VII. CONCLUSION

38. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Matthew T. Curtis

Matthew Curtis, Affiant
Special Agent, IRS Criminal Investigations

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The items to be searched are:

a. An Apple Iphone, black in color, inside a clear case, recovered from defendant MAKAIO LYMAN CRISLER at the time of his arrest on December 8, 2022, and which phone was used by MAKAIO LYMAN CRISLER at the time of his arrest to contact his wife; and

b. Apple Iphone mini, black in color, inside a black leather case, recovered from the pocket of defendant RICHARD SCOTT NEMROW at the time of his arrest on December 8, 2022, and which phone had, inside the case, cards belonging to defendant RICHARD SCOTT NEMROW.

(collectively, the "Devices"). The Devices are currently in the possession of law enforcement in the evidence storage room at 324 25th Street, Ogden, UT 84401.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 1344 (Conspiracy to Commit Bank Fraud), 18 U.S.C. § 1957 (Conspiracy to Commit Money Laundering); 18 U.S.C. § 1343 (Wire Fraud), and 18 U.S.C. § 1028A (Aggravated Identity Theft), for the time period January 1, 2016, through the present, including:

a. Communications or other records concerning the creation of LLCs, businesses, other legal entities;

b. Communications or other records concerning bank accounts, merchant accounts, merchant processing accounts, and underwriting or due diligence for such accounts;

c. Communications or other records concerning the creation or modification of websites for LLCs, businesses, or other legal entities;

d. Communications, recordings (video or audio), or photographs with or involving any indicted defendant, owner, or employee of Target Fulfillment, Total Client Connect DBA for Elite Business Resources LLC, Energia LLC, and/or Control Marketing LLC;

e. Communications or other records concerning the use or modification of a customer relationship management software program or "CRM";

f. Communications with any owner or straw owner of any business entity that attempted to or obtained a merchant processing account;

g. Communications with any entity or individual that assisted in obtaining or managing merchant processing accounts;

h. Communications or other records concerning chargebacks, disputed transactions, or "friendlies" (i.e., any transaction designed to manipulate or to lower the chargeback rate);

i. Communications or other records concerning the creation of email addresses purporting to belong to or be controlled by any of the sham LLCs or straw owners, and any communications to, from, on or behalf of these email addresses;

j. Communications or other records concerning the purchase, advertising, or sale of nutraceutical CBD, or dietary supplement products;

k. Communications or other records concerning consumer complaints relating to the purchase, advertising, or sale of any nutraceutical, CBD, or dietary supplement products or any business entity through which such products were purchased, advertised, or sold;

l. Communications or other records concerning bank accounts and other financial records;

m. Communications or other records concerning the transfer of money to or among the indicted defendants or any third parties;

n. Communications or other records concerning any indicted defendant's knowledge of a criminal investigation into their conduct;

2. Evidence indicating how and when the Devices were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account user;

3. Evidence indicating the state of mind of the Device user as it relates to the crimes under investigation;

4. Evidence of the identity of the person(s) who used the Devices;

5. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, text messages, instant messaging, electronic mail, documents, and browsing history;

6. Passwords, encryption keys, and other access devices that may be necessary to access the Devices;

7. Records of or information about Internet Protocol addresses used by the Devices; and

8. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

For purposes of this attachment, "indicted defendant" refers to APRIL GREN BAWDEN, CHAD AUSTIN BAWDEN, MAKAIO LYMAN CRISLER, PHILLIP GANNUSCIA, DUSTIN GARR, BARBARA JO JACKSON, BRENT GOLDBURN KNUDSON, ROBERT MCKINLEY, and RICHARD SCOTT NEMROW, each of whom are named in the indictment in case number 2:22-cr-00481-CW, which is pending in the United States District Court for the District of Utah.